

THE SIMPLEST TYPE OF ANALYTIC RANK OF TWISTED CARLITZ MODULES

D. LOGACHEV

ABSTRACT. The analytic rank under consideration is the order of 0 at $U = 1$ of the L -function of the simplest type $L(\phi, U)$ of a Drinfeld module ϕ of rank 1 over $\mathbb{F}_q[\theta]$. These Drinfeld modules are the twisted Carlitz modules. A version of the Lefschetz trace formula gives us an explicit expression of $L(\phi, U)$. We get immediately that there exists a coset of index $(q-1)^2$ in $\text{Hom}(\text{Gal}(\mathbb{F}_q(\theta)), \mathbb{Z}/(q-1))$ — the set of all twists — such that the analytic rank of corresponding Drinfeld modules is ≥ 1 . We present results of computer calculations of rank for the case $q = 3$ which show that there are examples of twists whose rank is ≤ 3 . It is unknown whether there exist examples of higher rank.

Standard reference for T-motives is [A], we use its notations. Let q be a power of a prime p . The Anderson ring $\mathbb{F}_q(\theta)[T, \tau]$ is the ring of non-commutative polynomials over $\mathbb{F}_q(\theta)$ satisfying the following relations:

$$T\theta = \theta T, \quad T\tau = \tau T, \quad \tau\theta = \theta^q\tau$$

We need the following (less general than in [A]) version of the definition of Anderson T-motives M over $\mathbb{F}_q(\theta)$:

Definition. An Anderson T-motive M is a $\mathbb{F}_q(\theta)[T, \tau]$ -module such that

- (1) M considered as a $\mathbb{F}_q(\theta)[T]$ -module is free of finite dimension r ;
- (2) M considered as a $\mathbb{F}_q(\theta)[\tau]$ -module is free of finite dimension n ;
- (3) $(T - \theta)M/\tau M = 0$.

Equivalently, we can consider M as a free finite-dimensional $\mathbb{F}_q(\theta)[T]$ -module endowed with a map $\tau : M \rightarrow M$ satisfying $\tau(\theta m) = \theta^q \tau(m)$, $\tau(Tm) = T\tau(m)$ such that conditions equivalent to (2), (3) hold.

There are various kinds of L -series of M , we consider the simplest type of L -series defined for example in [L], end of page 5 (τ , u , T of [L] are respectively fr , τ , U of the present paper. Sorry.) Its explicit definition is the following. Let $Q \in M_{r \times r}(\mathbb{F}_q(\theta)[T])$ be the matrix of multiplication by τ in a $\mathbb{F}_q(\theta)[T]$ -basis of M . Let \mathfrak{P} be an irreducible polynomial in $\mathbb{F}_q[\theta]$. M is called good at \mathfrak{P} if there exists a $\mathbb{F}_q(\theta)[T]$ -basis of M such that all entries of Q are integer at \mathfrak{P} . The set of bad primes is denoted by S .

We need the following notation. For $a \in (\mathbb{F}_q[\theta]/\mathfrak{P})[T]$, $a = \sum c_i T^i$ where $c_i \in \mathbb{F}_q[\theta]/\mathfrak{P}$, we denote $a^{(k)} := \sum c_i^{q^k} T^i$, $a^{[k]} := a^{(k-1)} \cdot \dots \cdot a^{(1)} \cdot a$ and for a matrix $A = (a_{ij}) \in M_{r \times r}((\mathbb{F}_q[\theta]/\mathfrak{P})[T])$ $A^{[k]} := (a_{ij}^{[k]})$.

The local \mathfrak{P} -factor $L_{\mathfrak{P}}(M, U)$ is defined as follows ($\mathfrak{P} \notin S$). Let d be the degree of \mathfrak{P} and $\tilde{Q} \in M_{r \times r}((\mathbb{F}_q[\theta]/\mathfrak{P})[T])$ the reduction of Q at \mathfrak{P} . We have:

$$L_{\mathfrak{P}}(M, U) := \det(E_r - \tilde{Q}^{[d]} U^d)^{-1} \in \mathbb{F}_q[T][[U^d]]$$

(because obviously $\det(E_r - \tilde{Q}^{[d]} U) \in \mathbb{F}_q[T, U]$);

$$L_S(M, U) := \prod_{\mathfrak{P} \notin S} L_{\mathfrak{P}}(M, U) \in \mathbb{F}_q[T][[U]]$$

A twisted Carlitz module M is an Anderson T-motive having $r = n = 1$. Let $\{e\} = \{e_1\}$ be the only element of a basis of M over $\mathbb{F}_q(\theta)[\tau]$. There exists $P_0 \in \mathbb{F}_q(\theta)$ such that the action of T on e is given by the equation $Te = \theta e + P_0 \tau e$. We denote this M by $\mathfrak{C}(P_0)$. Two such modules $\mathfrak{C}(P_{01})$, $\mathfrak{C}(P_{02})$ are isomorphic over $\mathbb{F}_q(\theta)$ iff $P_{01}/P_{02} \in \mathbb{F}_q(\theta)^{*(q-1)}$. So, we can consider only the case $P_0 = P^{-1}$ where $P \in \mathbb{F}_q[\theta]$, we denote this module by \mathfrak{C}_P .

The matrix $Q(\mathfrak{C}_P)$ consists of one element $P(T - \theta)$, hence $S = \emptyset$.

Let $P = \sum_{i=0}^m a_i \theta^i$, $a_i \in \mathbb{F}_q$. We denote by $M(P, k)$ (here k is sufficiently large) the matrix in $M_{k \times k}(\mathbb{F}_q[T])$ defined by the formula

$$M(P, k)_{i,j} = a_{iq-j} T - a_{iq-j-1} \quad (4)$$

(here $a_* = 0$ if $*$ $\notin [0, \dots, m]$):

$$M(P, k) = \begin{pmatrix} a_{q-1}T - a_{q-2} & a_{q-2}T - a_{q-3} & \dots & a_{q-k}T - a_{q-k-1} \\ a_{2q-1}T - a_{2q-2} & a_{2q-2}T - a_{2q-3} & \dots & a_{2q-k}T - a_{2q-k-1} \\ a_{3q-1}T - a_{3q-2} & a_{3q-2}T - a_{3q-3} & \dots & a_{3q-k}T - a_{3q-k-1} \\ \dots & \dots & \dots & \dots \\ a_{kq-1}T - a_{kq-2} & a_{kq-2}T - a_{kq-3} & \dots & a_{kq-k}T - a_{kq-k-1} \end{pmatrix} \quad (5)$$

Proposition 6. $L(\mathfrak{C}_P, U)$ is the stable value of $\det(E_k - M(P, k)U)$ as $k \rightarrow \infty$ (more exactly, for any $k \geq \frac{m+1}{q-1}$, see below).

This follows immediately from the Lefschetz trace formula (see for example (1) of [L], page 6). Before giving a proof, we need some definitions. The Lefschetz trace formula holds for a slightly different object called \mathcal{E} - τ -sheaf ([L], page 5). Let us recall its definition in the form that we need. Let P^1 be the projective line over \mathbb{F}_q with the function field $\mathbb{F}_q(\theta)$ and $\text{fr} : P^1 \rightarrow P^1$ the Frobenius map. The map $(\text{fr}, \text{Id}) : P^1 \times \text{Spec } F_q[T] \rightarrow P^1 \times \text{Spec } F_q[T]$ is denoted by fr as well.

Definition. A \mathcal{E} - τ -sheaf¹ is a pair (\mathcal{E}, τ) where \mathcal{E} is a locally free sheaf on $P^1 \times \text{Spec } F_q[T]$ and τ is a $P^1 \times \text{Spec } F_q[T]$ -linear map $\text{fr}^*(\mathcal{E}) \rightarrow \mathcal{E}$.

¹This is a particular case of the general definition of [L].

Let $U_0 = P^1 - \{\infty\}$, $U_\infty = P^1 - \{0\}$ be Zariski open subsets of P^1 .

Remark. We do not require that the restrictions of (\mathcal{E}, τ) to $U_0 \times \text{Spec } F_q[T]$, $U_\infty \times \text{Spec } F_q[T]$ satisfy (2), (3), because we do not need this assumption.

The definition of L extends to \mathcal{E} - τ -sheaves; clearly the product includes the point $\infty \in P^1$, and — because τ is Zariski-locally over $\mathbb{F}_q[\theta, T]$ (and not over $\mathbb{F}_q(\theta)[T]$) — we see that the set of bad points S is empty.

We need also a skew map $\varphi : \mathcal{E} \rightarrow \text{fr}^*(\mathcal{E})$ (it is denoted by τ in [L], p.6, line 5). For the affine case its definition is the following. Let $X = \text{Spec } A$, L a coherent sheaf on X corresponding to an A -module M . The sheaf $\text{fr}^*(L)$ corresponds to the module $M \otimes_A A$ respectively the Frobenius map $A \rightarrow A$. At the level of modules the map $\varphi : M \rightarrow M \otimes_A A$ is defined by $m \mapsto m \otimes 1$; we have $\varphi(am) = am \otimes 1 = m \otimes a^{(1)} = a^{(1)}\varphi(m)$. This definition obviously extends to the case of any scheme, as well as to cohomology.

Theorem (Lefschetz trace formula)

$$L(\mathcal{E}, \tau, U) = \frac{\det(1 - H^1(P^1, \tau \circ \varphi) \cdot U)}{\det(1 - H^0(P^1, \tau \circ \varphi) \cdot U)} \quad (7)$$

Proof of Proposition 6. To apply (7) to $L(\mathfrak{C}_P, U)$ we should construct firstly

(8) a \mathcal{E} - τ -sheaf whose restriction to $U_0 \times \text{Spec } F_q[T]$ is \mathfrak{C}_P .

Let $\mathcal{E} = \pi^*(O(n))$ where $\pi : P^1 \times \text{Spec } F_q[T] \rightarrow P^1$ is the projection. We have $\text{fr}^*(\mathcal{E}) = \pi^*(O(qn))$. We denote by e_i (resp. f_i), $i = 0, 1$, the only element of a basis of $\mathcal{E}(U_i \times \text{Spec } F_q[T])$ (resp. $\text{fr}^*(\mathcal{E})(U_i \times \text{Spec } F_q[T])$) over $O(U_i \times \text{Spec } F_q[T])$, so $e_1 = \theta^n e_0$ in $\mathcal{E}((U_0 \cap U_1) \times \text{Spec } F_q[T])$, $f_1 = \theta^{qn} f_0$ in $\text{fr}^*(\mathcal{E})((U_0 \cap U_1) \times \text{Spec } F_q[T])$. Condition (8) implies $\tau(f_0) = P(T - \theta)e_0$, hence

$$\tau(f_1) = \theta^{(q-1)n} P(T - \theta)e_1 \quad (9)$$

In order to get a map $\tau : \text{fr}^*(\mathcal{E}) \rightarrow \mathcal{E}$, we must have $\theta^{(q-1)n} P(T - \theta) \in \mathbb{F}_q[\theta^{-1}, T]$, which is equivalent $n \leq -\frac{m+1}{q-1}$. We fix one such n and hence \mathcal{E} .

It is clear that $\varphi : \mathcal{E} \rightarrow \text{fr}^*(\mathcal{E})$ is defined by the formulas $\varphi(e_i) = f_i$, $i = 0, 1$.

We denote $k = -n - 1$. We have $H^0(\mathcal{E}) = 0$, and elements $\theta^{-1}e_0, \dots, \theta^{-k}e_0$ form a basis of $H^1(\mathcal{E})$. We have $\varphi(\theta^{-i}e_0) = \theta^{-qi}f_0$ and

$$\tau \circ \varphi(\theta^{-i}e_0) = \theta^{-iq} P(T - \theta)e_0 = \sum_j (a_{iq-j}T - a_{iq-j-1})\theta^{-j}e_0$$

hence for $n \leq -\frac{m+1}{q-1}$ we have $L(\mathcal{E}, \tau, U) = \det(E_k - M(P, k)U)$.

Finally,

$$L(\mathcal{E}, \tau, U) = L(\mathfrak{C}_P, U) \cdot L_\infty(\mathcal{E}, \tau, U) \quad (10)$$

We have $L_\infty(\mathcal{E}, \tau, U) = 1$ if $n \neq -\frac{m+1}{q-1}$ and

$$L_\infty(\mathcal{E}, \tau, U) = (1 + a_m U)^{-1} \text{ if } n = -\frac{m+1}{q-1} \quad (11)$$

(This follows immediately from (7), or it can be calculated explicitly as follows. (9) is written as

$$\tau(f_1) = \left[\sum_{i=0}^m a_i \cdot (\theta^{-1})^{-(q-1)n-i} \cdot T - \sum_{i=0}^m a_i \cdot (\theta^{-1})^{-(q-1)n-i-1} \right] e_1 \quad (12)$$

The reduction at infinity gives us $\theta^{-1} \mapsto 0$, the only term in (12) containing $(\theta^{-1})^0$ is the term $-a_m$ corresponding to $i = m = -(q-1)n - 1$ in the second sum).

In all cases we get the formula for $L(\mathfrak{C}_P, U)$ (it is clear that $\det(E_k - M(P, k)U)$ does not depend on k for $k \geq \frac{m+1}{q-1}$, see also proof of Proposition 16). \square

Remark 13. If $P_1 = PQ^{q-1}$ for $Q \in \mathbb{F}_q[\theta]$ then $\mathfrak{C}_P, \mathfrak{C}_{P_1}$ are different $F_q(\theta)$ -models of a twisted Carlitz module over $\mathbb{F}_q(\theta)$, hence their L -series differ by a factor corresponding to bad points — irreducible factors of Q which do not enter in P . If $Q = \prod_i \mathfrak{Q}_i^{\alpha_i} \cdot \prod_j \mathfrak{Q}'_j{}^{\alpha'_j}$ is the prime decomposition of Q (where \mathfrak{Q}_i do not divide P and $\mathfrak{Q}'_j | P$), then

$$L(\mathfrak{C}_{P_1}, U) = L(\mathfrak{C}_P, U) \left(\prod_i L_{\mathfrak{Q}_i}(\mathfrak{C}_P, U) \right)^{-1} \quad (14)$$

Remark 15. I do not know a direct proof of (14) in terms of the characteristic polynomials of (5), without using of (7). This relation holds only in characteristic p , not 0.

The analytic rank of \mathfrak{C}_P is the multiplicity of the root $U = 1$ of $L(\mathfrak{C}_P, U)$, it does not depend on the factor Q^{q-1} . We have a trivial case when $r \geq 1$:

Proposition 16. If $m \equiv -1 \pmod{q-1}$ and $a_m = -1$ then $r \geq 1$.

Proof. Follows immediately from (10), (11). More explicitly, let $i = \frac{m+1}{q-1}$. For $j \geq i$ all elements on the j -th line of $E_k - M(P, k)U$ to the left from the diagonal are 0, and the diagonal element $(E_k - M(P, k)U)_{jj}$ is 1 for $j > i$, and it is $1 + a_m U$ for $j = i$. This means that $1 + a_m U$ is a factor of $\det(E_k - M(P, k)U)$. \square

This case corresponds to a coset. Namely, the set of twists of \mathfrak{C} is isomorphic to $\text{Hom}(\text{Gal}(\mathbb{F}_q(\theta)), \mathbb{Z}/(q-1))$. This is a free $\mathbb{Z}/(q-1)$ -module generated by $i_0, i_{\mathfrak{Q}}$ where i_0 comes from \mathbb{F}_q^* and \mathfrak{Q} runs over the set of places of $\mathbb{F}_q[\theta]$. Let us consider a homomorphism ϕ of this group to $[\mathbb{Z}/(q-1)]^2 = [\mathbb{Z}/(q-1)]j_1 \oplus [\mathbb{Z}/(q-1)]j_2$ defined as follows: $i_0 \mapsto j_1, i_{\mathfrak{Q}} \mapsto \deg(\mathfrak{Q})j_2$.

Proposition 17. The set of twists of Proposition 16 is $\phi^{-1}(\frac{q-1}{2}j_1; -j_2)$ for odd q and $\phi^{-1}(0 \cdot j_1; -j_2)$ for even q , i.e. it is a coset of a subgroup of index $(q-1)^2$ of the group of twists. \square

Recall the corresponding fact for the number field case. Let E be an elliptic curve over \mathbb{Q} , E' its twist corresponding to an element $\alpha \in \text{Hom}(\text{Gal}(\mathbb{Q}), \text{Aut}(E))$. There exists a subgroup G_0 of index 2 in $\text{Hom}(\text{Gal}(\mathbb{Q}), \text{Aut}(E))$ such that the parity of the analytic rank of E' coincides (resp. does not coincide) with the one of E if $\alpha \in G_0$ (resp. $\alpha \notin G_0$).

Let us try to predict the maximal value of the analytic rank of \mathfrak{C}_P , $P \in \mathbb{F}_q[\theta]$, using the naive parameter count (quantity of variables and quantity of equations).

Changing variable $V = U^{-1}$ we get $L(\mathfrak{C}_P, U) = V^{-k} \sum_{i=0}^k C_i V^i$ where $C_i \in \mathbb{F}_q[T]$, $\deg C_i = k - i$ where k is the size of $M(P, k)$. Changing variable $V = \bar{V} + 1$ we get $L(\mathfrak{C}_P, U) = V^{-k} \sum_{i=0}^k \bar{C}_i \bar{V}^i$ where $\bar{C}_i \in \mathbb{F}_q[T]$, $\deg \bar{C}_i = k - i$. Condition that the analytic rank is $\geq r_0$ is equivalent to the condition $\bar{C}_0 = \dots = \bar{C}_{r_0-1} = 0$, which gives us

$$(k+1) + (k) + \dots + (k+1 - (r_0 - 1)) = r_0(k+1) - \frac{r_0(r_0 - 1)}{2} \quad (18)$$

equations in \mathbb{F}_q , where $r_0 \leq k$.

Let us find the maximal value of r for which we can find k such that the naive parameter count predicts existence of $k \times k$ matrix of analytic rank r . We take $m = kq - k - 1$, $a_{kq-k-1} = -1$, hence the last line of $\det(E_k - M(P, k)U)$ gives us a factor $(1 - U)$. Formula (18) applied to the left-upper $(k-1) \times (k-1)$ -minor of $M(P, k)$, $r_0 = r - 1$, gives us $(r-1)k - \frac{(r-1)(r-2)}{2}$ equations. The quantity of variables a_i is $k(q-1) - 1$, hence the question is the following:

19. For which r there exists $k \geq r$ such that

$$k(q-1) - 1 \geq (r-1)k - \frac{(r-1)(r-2)}{2} \quad (20)$$

The answer on (19) is $r \leq 2q - 3$, this is the expected maximal value of rank.

Analogously, we can ask for which r there exist infinitely many k satisfying (20), i.e. for which r we can expect existence of infinitely many P such that the analytic rank of \mathfrak{C}_P is $\geq r$. The answer is $r \leq q$.

Clearly this parameter count does not take into consideration the formula (14).

Let us mention the following elementary result:

Proposition 21. For any $r \leq q - 1$ there exists P such that the analytic rank of \mathfrak{C}_P is r .

Proof. We can take for example P having $a_{i(q-1)-1} = -1$ for $i = 1, \dots, r$ and other $a_* = 0$. The matrix $M(P, k)$, where $k = r$, is upper-triangular with 1's at the diagonal, hence the proposition. \square

Results of computer calculations for $q = 3$ are given in the following tables. We consider squarefree $P \in \mathbb{F}_3[\theta]$ of degree $m \leq 13$. Tables give the quantity of these P such that the analytic rank of \mathfrak{C}_P is 2 and 3 (rank ≥ 4 does not occur for $m \leq 13$; if $m < 3$ then rank = 0 or 1). We give separately the cases of the leading coefficient $a_m = 1$ and 2.

Rank 2												
a_m	$m =$	3	4	5	6	7	8	9	10	11	12	13
1		0	0	0	0	0	3	0	0	3	9	12
2		3	0	0	0	33	3	159	0	717	9	> 1000

Rank 3												
1		0	0	0	0	0	0	3	0	0	0	0
2		0	0	0	0	0	0	6	0	0	0	12

The above parameter count predicts that we should have $\sim 3^{(m-1)/2}$ polynomials of rank 2 having m odd, $a_m = 2$, as well as polynomials of rank 1 having m even or $\{m \text{ odd}, a_m = 1\}$, and a bounded (or slowly growing) quantity of polynomials of rank 3 having m odd, $a_m = 2$, as well as polynomials of rank 2 having m even or $\{m \text{ odd}, a_m = 1\}$. We see that the results of calculations are in concordance with these predictions. More exactly, we have $\sim (\frac{m-1}{2} - 2) \cdot 3^{(m-1)/2}$ polynomials of rank 2 having m odd, $a_m = 2$; the coefficient $\frac{m-1}{2} - 2$ is not explained by the parameter count.

Let us formulate now some questions.

1. Do other sets of twists having rank > 0 have a description similar to the one of Proposition 17?

2. Do we really have that the maximal value of r is $2q - 3$ and the maximal value of r such that there exists infinitely many P such that the analytic rank of \mathfrak{C}_P is r , is q ?

3. Why all numbers in the above tables are multiples of 3? If we consider polynomials of degree $\leq m$ as points in \mathbb{F}_3^{m+1} (coefficients are coordinates) then some sets of 3 (resp. 9) elements in the above tables are not straight lines (resp. unions of straight lines). For bigger q we shall be able to check whether the analogous sets of q, q^2 etc. points belong to a conic line, an affine plane etc., or not.

References

- [A] Anderson, Greg W. t -motives. Duke Math. J. 53 (1986), no. 2, 457 – 502
- [L] Lafforgue, Vincent. Valeurs spéciales des fonctions L en caractéristique p . J. Number Theory 129 (2009), no. 10, 2600 – 2634

DEPARTAMENTO DE MATEMÁTICAS UNIVERSIDAD SIMÓN BOLÍVAR APARTADO POSTAL 89000
CARACAS, VENEZUELA AND INSTITUTE FOR APPLIED MATHEMATICS, KHABAROVSK DIVISION
680000, 92 ZAPARINA STR., KHABAROVSK CITY, RUSSIA